REMARKS

Reconsideration of this application and allowance of the claims is respectfully requested.

REJECTIONS UNDER 35 U.S.C. §112

The Examiner's rejections of Claims 21-23 under 35 U.S.C. 112 have been carefully considered but they are believed to be clearly erroneous. All of the claimed subject matter of Claims 21-23 is fully disclosed in the present application. The present application concerns a novel method for creating a player identification usable in the gaming environment and having at least two authenticators. Applicant's first and second authenticators are similar to the first and second authenticators described in *Bradford et al.* U.S. Patent No. 6,612,928, from where Claims 21-23 were derived. As pointed out in the Amendment filed October 10, 2003 with a Request for Interference, Claim 21 corresponds substantially to Claim 1 of the '928 Patent; Claim 22 corresponds substantially to Claim 2 of the '928 Patent; and Claim 23 corresponds exactly to Claim 32 of the '928 Patent.

In the '928 Patent, the first authenticator is defined as whatever a player first presents to the system to identify themselves. The second authenticator is a biometrically-based authentication. Likewise, in the present application, the first authenticator is created when the player approaches a registration desk and requests a smart card (a BDSD). To this end, the registration entity creates the first authenticator by obtaining personal and financial information from the player such as name, address, social security or tax ID, local hotel or other address, credit card or bank account information and the like. See page 4 of the present application, line 29 to page 5, line 6.

Page 6 line 1+ also lists information that can be stored on the smart card, showing how the first authenticator is created.

On page 15 of the office action, the Examiner states that the Section 112 rejection is maintained because the specification does not describe "***the creation*** of authenticator(s)". However, creation of the authenticators is very clearly disclosed in the present application where it is stated that the personal information of the player is encrypted onto a smart card. The specific process of encrypting information onto a smart card was very well known in the art prior to Applicant's invention.

As in the '928 Patent, the second authenticator in the present invention is a biometrically-based authentication means. For example, a second authenticator in the present application is described in page 5 lines 17-20, as well as many other places throughout the specification in which it is described how biometric information is obtained.

The second authorization is also described in column 6, line 20 to column 7, line 12. The gaming terminal includes a smart card reader for reading the biometric reference data from the BDSD and also includes data processing capabilities including microprocessors. The gaming terminal includes a device for obtaining biometric data from the player such as a finger or thumbprint scan device. The data measured at the terminal is compared to reference data from the BDSD and if there is match the second authorization is accepted. This allows an electronic transfer of funds in that the player can access his or her account and/or use the debit card balance. See page 7, lines 3-5. Page 7, lines 13 and 14 bring out how the players wagers are charged to, and all of the

players prizes or winnings are credited to, the player's account and/or debit card balance. This is an electronic fund transfer.

On page 10, lines 5-10, there is a discussion of how the biometric data can be measured without comparing to reference data stored on a card or other BDSD. Instead, the measured data can be compared to data stored in a central computer or other central repository. On lines 10-15, it discusses how an individual who has previously registered his biometric data with a casino or other registry can have the biometric data verified by comparing the measurement to a centralized data base. On page 10, line 15-18 it points out how the two authentications are required; first an authenticated PIN, password or similar code, and then authenticated biometric data.

The Examiner has rejected Claim 23 under 35 U.S.C. 112 because of an alleged problem with the words "electronic transfer". However, from viewing the Examiner's statement on page 15 of the Office Action, it appears there is a possible misunderstanding with respect to "electronic transfer". In both the present application and in the '928 Patent, "electronic transfer" does not refer to the transfer of goods from the gaming device to the user, or of user information from the user to the gaming device, or both. Instead, it refers to electronic money transfer. For example, referring to Figure 12 of the '928 Patent and its associated disclosure, the electronic transfer is the Automated Electronic Funds transfer. In the present application, as stated above, once (a) the first authenticator is read by the gaming device, (b) the second authenticator (biometric information) is read by the gaming device and the player is recognized in the player identification database, ***the electronic transfer of funds can occur***. See, for example, page 7, line 2-5 and page 12, lines 14-26.

In short, both the present application and the '928 Patent recognize a player based on a first authenticator and a second authenticator (which second authenticator is biometric) and then when the player is identified by associating the first authenticator with the second authenticator, the electronic transfer of funds becomes available. All of the claimed subject matter of Claims 21-23 is fully disclosed in the present application the Section 112 rejections should be withdrawn.

For the Examiner's convenience, the following is a chart outlining the specification support for Claims 21-23:

21. A method for creating a player identification usable in a gaming environment and having at least two authenticators, the method comprising:	Page 1, 2d paragraph Page 6, lines 1-4
(a) creating a first authenticator;	Page 4, line 29 - Page 5, line 6 Page 5, lines 1-6 Page 6, lines 1-4
(b) entering at least one more authenticator in the form of biometric data;	Page 3, lines 16-25 Page 5, lines 1-2 and 11-16 Page 6, line 20 - Page 7, line 12
(c) associating said first authenticator and said at least one more authenticator with a player;	Page 4, line 29 – Page 5, line 6
(d) providing player identification at a game device having an associated biometric reader using said first authenticator and at least one of said at least one more authenticators, where said first authenticator is a data storage device.	Page 6, lines 1-4; line 25 to page 6, line 8 Page 3, lines 22-25 Page 10, lines 5-18 Page 12, lines 1-3
22. A method for creating a player identification usable in a gaming environment and having at least two authenticators, the method comprising:	Page 1, 2d paragraph Page 6, lines 1-4

(a) creating a first authenticator;	Page 4, line 29 - Page 5, line 6 Page 5, lines 1-6 Page 6, lines 1-4
(b) entering at least one more authenticator in the form of biometric data;	Page 3, lines 16-25 Page 5, lines 1-6 Page 6, line 20 - Page 7, line 12
(c) associating said first authenticator and said at least one more authenticator with a player and further identifying said first authenticator as an authenticator that will be the authenticator used for searching and identifying said player in a player identification database; and	Page 4, line 29- page 5, line 6 Page 10, lines 5-18
(d) providing player identification at a game device having an associated biometric reader using said first authenticator and at least one of said at least one more authenticators.	Page 6, lines 1-4; line 25 to page 6, line 8 Page 3, lines 22-25 Page 10, lines 14-18 Page 12, lines 1-3
23. A method for enabling electronic transfers using at least two authenticators where any authenticator that is not the first authenticator uses biometric data, in a gaming environment while using a game device having an associated biometric reader, the method comprising:	Page 5, lines 1-6 and 17-28 Page 6, lines 1-4 and 9-11 and 20- page 7, line 8
(a) having a first authenticator readable by a reader associated with said game device;	Page 4, line 29 – Page 5, line 6 Page 6, lines 1-4 and 20-25 Page 5, lines 1-6
(b) having a second authenticator different from said first authenticator and readable by a reader associated with said game device;	Page 5, lines 1-6; 11-14 Page 3, lines 16-25 Page 6, line 20 – Page 7, line 12
(c) having an entry in a player identification database, where said entry further comprises first authenticator data and second authenticator data;	Page 6, lines 1-4 Page 10, lines 5-10 Page 12, lines 14-26

(d) uniquely associating a player using a game device with an entry in said player identification database and recognizing a player request for an electronic transfer;	Page 6, lines 9-11 and 20 – page 7, line 8
(e) acknowledging a desired electronic transfer;	Page 6, lines 9-11 Page 6, line 29 – page 7, line 2 Page 12, lines 14-26
(f) using said second authenticator to confirm and authorize said desired electronic transfer.	Page 7, lines 2-5 Page 7, lines 13-14 Page 12, lines 14-26

REJECTIONS UNDER 35 U.S.C. §103(a)

In order to expedite prosecution of this application, claims 15-19 have been cancelled and independent claims 1, 8, and 24 have been amended to more clearly distinguish applicant's invention over the prior art references.

As set forth in claim 1, for example, the present invention concerns a gaming apparatus which comprises a portable biometric data storage device storing biometric data for a player. The biometric data storage device comprises a debit card that is carried by the player separate from the gaming apparatus. The apparatus includes a gaming terminal which is configured for playing at least a first game. A reader is coupled to the gaming terminal and receives the biometric data stored on the debit card. The gaming apparatus includes a biometric measuring device for measuring the biometric data of the player. The measured biometric data of the player is compared to the stored biometric data and if there is a match, there is an output of an authorization allowing the player to access his or her account and/or use the debit card balance to play the gaming apparatus.

The prior art does not teach applicant's invention. Schneier et al. concerns a method and apparatus for securing electronic games. As the Examiner acknowledges, Schneier does not disclose the concept of a portable biometric data storage device comprising a debit card. Nowhere does Schneier disclose, teach or even suggest any portable storage device that is carried by a player. In fact, Schneier teaches away from using a portable debit card carrying the biometric information, because in Schneier, the information is already stored in a database.

As a purported teaching of "a portable biometric storage device" the Examiner refers to column 4, lines 47-57, which mentions "optical storage units". However, the "optical storage units" and the data storage devices described in Schneier are not portable devices carried by a player separate from the gaming apparatus but instead comprise hardware that in the gaming apparatus server. This is contrary to the intention of applicant's claimed invention, where the player carries a debit card having biometric data, which debit card is separate from the gaming apparatus.

Applicant's invention enables a player to effectively maintain possession and control of his or her biometric information on a debit card carried by the player separate from the gaming apparatus. This use of a portable debit card which the player can readily retain in his or her possession and under his or her control is extremely important, because in the gaming environment a player often does not want his or her biometric information to be stored in a central computer or in a server or in the gaming apparatus itself. Schneier discloses exactly what the present invention is intended to avoid, wherein a player's biometric information is stored on a server.

Applicant's claims have been carefully drafted to make it clear that applicant's system utilizes a portable biometric data storage device carried by the player which biometric data storage device comprises a debit card carried by the player separate from the gaming apparatus. As stated above, Schneier teaches away from this significant invention now claimed by applicant.

The Sehr publication does not remedy any of the deficiencies of Schneier. Sehr discloses a ticketing system, where portable ticketing cards may be smart credit or debit cards, and which may carry biometric identification of the cardholders. Sehr's ticketing system is basically a system providing access to an event, and there is no disclosure, suggestion, or even hint of using the Sehr ticketing system in connection with a gaming apparatus. Particularly, when it is considered that Schneier's gaming apparatus already contains biometric storage in a server, there is no motivation for combining Sehr's ticketing system with Schneier's electronic game server. This is because nothing in Schneier indicates a desire for a portable debit card carrying biometric information, separated from the gaming apparatus, and nothing in Sehr suggests using Sehr's ticketing system in a gaming apparatus that already includes stored biometric data.

It is submitted that the combination of references raised by the Examiner fails to establish a *prima facie* case of obviousness.

As stated in MPEP §2142: "To establish a *prima facie* case of obviousness three basic criteria must be met. First there must be some suggestion or motivation either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or

references when combined) must teach or suggest all of the claim limitations. The teaching or suggestion to make the claim combination and the reasonable expectation of success must be found in the prior art, and not based on applicant's disclosure."

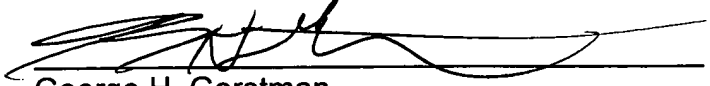
It can be seen that applicant has now presented claims that very clearly distinguish applicant's invention over the prior art references, whether taken singly or in combination with each other. Any possible combination of the Schneier and Sehr references are not based on anything taught by the references themselves, but would be based only upon hindsight after reading applicant's own disclosure.

In view of the foregoing, it is submitted that the claims as now presented are allowable over the prior art references. Further, the subject matter of claims 21-23 is fully disclosed in the present application and the Section 112 rejection should be withdrawn.

If for some reason the Examiner believes there are certain issues that needs to be discussed, the Examiner is requested to telephone counsel for applicant at (312) 269-8567.

Respectfully submitted,

SEYFARTH SHAW LLP



George H. Gerstman
Registration No. 22,419
Attorney for Applicant

SEYFARTH SHAW LLP
55 East Monroe Street, Suite 4200
Chicago, Illinois 60603
(312) 269-8567

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to: Mail Stop: Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on Dec. 8, 2005.

Registered Attorney for Applicant
Date: Dec. 8, 2005